

Shima
Filed 9/29/03
Q 77708
1 of 1

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 2 日
Date of Application:

出 願 番 号 特 願 2 0 0 2 - 2 9 0 3 8 7
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 2 9 0 3 8 7]

出 願 人 日 本 電 気 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 8 月 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 6 3 9 1 9

【書類名】 特許願

【整理番号】 65700120

【提出日】 平成14年10月 2日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00
H04L 9/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 島 成佳

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100102864

【弁理士】

【氏名又は名称】 工藤 実

【選任した代理人】

【識別番号】 100099553

【弁理士】

【氏名又は名称】 大村 雅生

【手数料の表示】

【予納台帳番号】 053213

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9715177

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子データ送受信システム

【特許請求の範囲】

【請求項 1】 ネットワークに接続され、第 1 番目から第 n 番目 (n は 2 以上の整数) までの n 個の装置と、

前記ネットワークに接続され、第 1 電子データを第 1 装置に送信する送信装置と、

前記ネットワークに接続され、第 n 装置からの第 $(n + 1)$ 電子データを受信する受信装置とを具備し、

第 j 装置 ($1 \leq j \leq n$ を満たす整数) は、自己を識別する署名を第 j 電子データに付与した第 $(j + 1)$ 電子データを生成して第 $(j + 1)$ 装置に送信し、

前記 j が前記 n のとき、第 $(n + 1)$ 装置は前記受信装置に対応する電子データ送受信システム。

【請求項 2】 請求項 1 に記載の電子データ送受信システムにおいて、

前記送信装置は、前記第 1 電子データと前記第 1 電子データの送信を認証する送信者認証子とを前記第 1 装置に送信し、

前記第 1 装置は、前記第 1 電子データと前記送信者認証子とに前記第 1 装置の署名を付与した第 2 電子データを生成して第 2 装置に送信する

電子データ送受信システム。

【請求項 3】 請求項 2 に記載の電子データ送受信システムにおいて、

更に、

送信装置用記憶装置を具備し、

前記第 1 装置は、前記第 1 電子データと前記送信者認証子とに前記第 1 装置の署名を付与した電子データである送信証拠データを生成して前記送信装置に送信し、

前記送信装置は、前記第 1 装置からの前記送信証拠データを前記送信装置用記憶装置に格納する

電子データ送受信システム。

【請求項 4】 請求項 2 又は 3 に記載の電子データ送受信システムにおいて、

前記第 n 装置は、第 $(n-1)$ 装置からの前記第 n 電子データを受信したとき、第 n 電子データ受信通知を前記受信装置に送信し、

前記受信装置は、前記第 n 電子データ受信通知に応じて、前記第 n 電子データの受信を認証する受信者認証子を前記第 n 装置に送信し、

前記第 n 装置は、前記第 n 電子データと前記受信者認証子とに前記第 n 装置の署名を付与した第 $(n+1)$ 電子データを生成して前記受信装置に送信する

電子データ送受信システム。

【請求項 5】 請求項 4 に記載の電子データ送受信システムにおいて、

更に、

受信装置用記憶装置を具備し、

前記受信装置は、前記第 n 装置からの第 $(n+1)$ 電子データを前記受信装置用記憶装置に格納する

電子データ送受信システム。

【請求項 6】 請求項 4 又は 5 に記載の電子データ送受信システムにおいて、

前記受信装置は、

前記送信者認証子と前記 n 個の装置の署名とが格納された受信装置用データベースを備え、

前記第 $(n+1)$ 電子データに付与された前記第 n 装置の署名を除いた前記第 n 電子データと前記受信者認証子とを取出し、

前記第 $(n+1)$ 電子データ及び前記第 2 電子データ以外の前記第 $(j+1)$ 電子データに付与された署名を除いた前記第 j 電子データを取出し、

前記第 2 電子データに付与された前記第 1 装置の署名を除いた前記第 1 電子データと前記送信者認証子とを取出し、

前記受信装置用データベースを参照して、前記送信装置が前記第 1 電子データを送信したことを認識する

電子データ送受信システム。

【請求項 7】 請求項 6 に記載の電子データ送受信システムにおいて、

前記第 1 装置は、前記送信装置から前記送信者認証子を受信した時刻を表す第 1 タイムスタンプに前記第 1 装置の署名を更に付与した前記第 2 電子データを生

成し、

前記第 n 装置は、前記受信装置から前記受信者認証子を受信した時刻を表す第 2 タイムスタンプに前記第 n 装置の署名を更に付与した前記第 $(n+1)$ 電子データを生成し、

前記受信装置は、

前記第 $(n+1)$ 電子データに付与された前記第 n 装置の署名を除いた前記第 n 電子データと前記受信者認証子と前記第 2 タイムスタンプとを取出し、

前記第 2 電子データに付与された前記第 1 装置の署名を除いた前記第 1 電子データと前記受信者認証子と前記第 1 タイムスタンプとを取出す

電子データ送受信システム。

【請求項 8】 請求項 4～7 のいずれか一項に記載の電子データ送受信システムにおいて、

前記第 n 装置は、前記第 n 電子データと前記受信者認証子とに前記第 n 装置の署名を付与した電子データである受信証拠データを生成して前記送信装置に送信する

電子データ送受信システム。

【請求項 9】 請求項 8 に記載の電子データ送受信システムにおいて、

前記送信装置は、

前記 n 個の装置の署名と前記受信者認証子とが格納された送信装置用データベースを備え、

前記受信証拠データに付与された前記第 n 装置の署名を除いた前記第 n 電子データと前記受信者認証子とを取出し、

前記受信証拠データ及び前記第 2 電子データ以外の前記第 $(j+1)$ 電子データに付与された署名を除いた前記第 j 電子データを取出し、

前記第 2 電子データに付与された前記第 1 装置の署名を除いた前記第 1 電子データと前記送信者認証子とを取出し、

前記送信装置用データベースを参照して、前記第 1 電子データが前記受信装置に送信されたことを認識する

電子データ送受信システム。

【請求項 1 0】 請求項 9 に記載の電子データ送受信システムにおいて、

更に、

第 1 電子データ記憶装置を具備し、

前記送信装置は、

前記第 1 電子データを送信する前に、前記第 1 電子データ記憶装置に前記第 1 電子データを格納し、

前記第 1 電子データを取り出したとき、前記第 1 電子データ記憶装置を参照して、前記第 1 電子データが改ざんされることなく前記受信装置に送信されたことを認識する

電子データ送受信システム。

【請求項 1 1】 請求項 1 0 に記載の電子データ送受信システムにおいて、

前記第 n 装置は、前記第 n 電子データと前記受信者認証子とに前記第 n 装置の署名を付与した電子データである受信証拠データを生成し、前記受信証拠データから前記第 1 電子データを削除した受信証拠データを前記送信装置に送信し、

前記送信装置は、前記第 n 装置からの前記削除された受信証拠データに、前記第 1 電子データ記憶装置に格納された前記第 1 電子データを付加して前記受信証拠データを復元する

電子データ送受信システム。

【請求項 1 2】 請求項 9 又は 1 1 に記載の電子データ送受信システムにおいて

、
前記第 1 装置は、前記送信装置から前記送信者認証子を受信した時刻を表す第 1 タイムスタンプに前記第 1 装置の署名を更に付与した前記第 2 電子データを生成し、

前記第 n 装置は、前記受信装置から前記受信者認証子を受信した時刻を表す第 2 タイムスタンプに前記第 n 装置の署名を更に付与した前記受信証拠データを生成し、

前記送信装置は、

前記受信証拠データに付与された前記第 n 装置の署名を除いた前記第 n 電子データと前記受信者認証子と前記第 2 タイムスタンプとを取出し、

前記第 2 電子データに付与された前記第 1 装置の署名を除いた前記第 1 電子データと前記受信者認証子と前記第 1 タイムスタンプとを取出す電子データ送受信システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、電子データ送受信システムに関し、特に、送信装置から送信された電子データが受信装置に受信されたか否かを確認する電子データ送受信システムに関する。

【0 0 0 2】

【従来の技術】

電子データ、電子文を送信するシステムが知られている（例えば、特許文献 1、特許文献 2、特許文献 3、特許文献 4 参照。）。

送信装置が中継機器を介して受信装置に電子データを送信するシステムでは、送信装置が受信装置に電子データを送信したとき、例えば、送信装置を利用する送信者は、送信装置が送信した電子データを受信装置が受信したか否かを確認するために、送信装置により中継機器と通信してログを収集する必要がある。送信装置が送信した電子データを受信装置が受信するまで保証するシステムが望まれる。

【0 0 0 3】

【特許文献 1】

特開 2 0 0 0 - 7 8 2 3 5 号公報

【特許文献 2】

特開 2 0 0 0 - 1 8 3 8 6 6 号公報

【特許文献 3】

特開 2 0 0 2 - 7 2 8 8 号公報

【特許文献 4】

特開 2 0 0 2 - 1 8 3 4 9 1 号公報

【0 0 0 4】

【発明が解決しようとする課題】

本発明の目的は、送信装置が送信した電子データを受信装置が受信するまで保証する電子データ送受信システムを提供することにある。

本発明の他の目的は、電子データが受信装置に送信された経路を検証することができる電子データ送受信システムを提供することにある。

本発明の更に他の目的は、電子データの改ざんを検出できる電子データ送受信システムを提供することにある。

本発明の更に他の目的は、ハッカーを防止する電子データ送受信システムを提供することにある。

【0005】**【課題を解決するための手段】**

以下に、[発明の実施の形態]で使用する番号・符号を用いて、課題を解決するための手段を説明する。これらの番号・符号は、[特許請求の範囲]の記載と[発明の実施の形態]の記載との対応関係を明らかにするために付加されたものであるが、[特許請求の範囲]に記載されている発明の技術的範囲の解釈に用いてはならない。

【0006】

本発明の電子データ送受信システムは、第1番目から第n番目（nは2以上の整数）までのn個の装置[5-1～5-n]と、送信装置[1]と、受信装置[2]とを具備する。n個の装置[5-1～5-n]と送信装置[1]と受信装置[2]とはネットワーク[100]に接続されている。送信装置[1]は、第1電子データを第1装置[5-1]に送信する。受信装置[2]は、第n装置[5-n]からの第(n+1)電子データを受信する。第j装置（ $1 \leq j \leq n$ を満たす整数）は、自己を識別する署名を第j電子データに付与した第(j+1)電子データを生成して第(j+1)装置に送信する。ここで、jがnのとき、第(n+1)装置は受信装置[2]に対応する。

電子データとしては、業者同士の業務に関する文書が記載された電子メールが例示され、その電子メールには画像が添付されている場合もある。また、電子データとしては、その業者同士の業務に関する電子データの他に、金融に関する電

子データ、民政に関する電子データが例示される。

本発明の電子データ送受信システムによれば、第 $(j + 1)$ 電子データが生成されるまでに付与された署名により、送信装置 [1] を用いて第 1 電子データを送信した送信者が第 1 電子データを送信していないと否認（送信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置 [1] が送信した第 1 電子データを受信装置 [2] が受信するまで保証する。

【0007】

本発明の電子データ送受信システムにおいて、第 j 装置が第 1 装置 [5-1] である場合、送信装置 [1] は、第 1 電子データと第 1 電子データの送信を認証する送信者認証子とを第 1 装置 [5-1] に送信する。第 1 装置 [5-1] は、第 1 電子データと送信者認証子とに第 1 装置 [5-1] の署名を付与した第 2 電子データを生成して第 2 装置 [5-2] に送信する。

本発明の電子データ送受信システムによれば、送信装置 [1] の署名に対応する送信者認証子と、第 $(j + 1)$ 電子データが生成されるまでに付与された署名とにより、送信装置 [1] を用いて第 1 電子データを送信した送信者が第 1 電子データを送信していないと否認（送信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置 [1] が送信した第 1 電子データを受信装置 [2] が受信するまで保証する。

【0008】

本発明の電子データ送受信システムは、更に、送信装置用記憶装置 [3] を具備する。第 1 装置 [5-1] は、第 1 電子データと送信者認証子とに第 1 装置 [5-1] の署名を付与した電子データである送信証拠データを生成して送信装置 [1] に送信する。送信装置 [1] は、送信装置 [1] は、第 1 装置 [5-1] からの送信証拠データを送信装置用記憶装置 [3] に格納する。

本発明の電子データ送受信システムによれば、第 1 装置 [5-1] の署名を付与した送信証拠データを送信装置用記憶装置 [3] に格納するため、送信装置 [1] を用いて第 1 電子データを送信した送信者が第 1 電子データを送信していないと否認（送信拒否）することができない。

【0009】

本発明の電子データ送受信システムにおいて、第 j 装置が第 n 装置 $[5-n]$ である場合、第 n 装置 $[5-n]$ は、第 $(n-1)$ 装置からの第 n 電子データを受信したとき、第 n 電子データ受信通知を受信装置 $[2]$ に送信する。受信装置 $[2]$ は、第 n 電子データ受信通知に応じて、第 n 電子データの受信を認証する受信者認証子を第 n 装置 $[5-n]$ に送信する。第 n 装置 $[5-n]$ は、第 n 電子データと受信者認証子とに第 n 装置 $[5-n]$ の署名を付与した第 $(n+1)$ 電子データを生成して受信装置 $[2]$ に送信する。

本発明の電子データ送受信システムによれば、送信者認証子と、第 $(j+1)$ 電子データが生成されるまでに付与された署名と、受信装置 $[2]$ の署名に対応する受信者認証子とにより、送信装置 $[1]$ を用いて第 1 電子データを送信した送信者が第 1 電子データを送信していないと否認（送信拒否）することができない。また、本発明の電子データ送受信システムによれば、受信装置 $[2]$ を利用する受信者が第 1 電子データを受取っていないと否認（受信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置 $[1]$ が送信した第 1 電子データを受信装置 $[2]$ が受信するまで保証する。

【0010】

本発明の電子データ送受信システムは、更に、受信装置用記憶装置 $[4]$ を具備する。受信装置 $[2]$ は、第 n 装置 $[5-n]$ からの第 $(n+1)$ 電子データを受信装置用記憶装置 $[4]$ に格納する。

第 $(n+1)$ 電子データは、送信者認証子と、 n 個の装置 $[5-1 \sim 5-n]$ の署名と、受信者認証子とが付与された第 1 電子データである。本発明の電子データ送受信システムによれば、第 $(n+1)$ 電子データを受信装置用記憶装置 $[4]$ に格納するため、受信装置 $[2]$ を利用する受信者が第 1 電子データを受取っていないと否認（受信拒否）することができない。

【0011】

本発明の電子データ送受信システムにおいて、受信装置 $[2]$ は、送信者認証子と n 個の装置 $[5-1 \sim 5-n]$ の署名とが格納された受信装置用データベース $[18]$ を備えている。受信装置 $[2]$ は、送信装置 $[1]$ が第 1 電子データを送信したことを検証する。受信装置 $[2]$ は、第 $(n+1)$ 電子データに付与

された第 n 装置 [5 - n] の署名を除いた第 n 電子データと受信者認証子とを取出す。受信装置 [2] は、第 $(n + 1)$ 電子データ及び第 2 電子データ以外の第 $(j + 1)$ 電子データに付与された署名を除いた第 j 電子データを取出す。受信装置 [2] は、第 2 電子データに付与された第 1 装置 [5 - 1] の署名を除いた第 1 電子データと送信者認証子とを取出す。受信装置 [2] は、受信装置用データベース [18] を参照して、送信装置 [1] が第 1 電子データを送信したことを認識する。

このように、本発明の電子データ送受信システムによれば、受信装置 [2] が第 $(n + 1)$ 電子データ、第 n 電子データ、…、第 2 電子データ、第 1 電子データの順で正しく確認（検証）できた場合、第 1 電子データは、送信装置 [1] によって送信されたことが保証される。また、本発明の電子データ送受信システムによれば、受信装置 [2] は、署名の履歴として第 1 電子データが受信装置 [2] に送信された経路（送信装置 [1]、 n 個の装置 [5 - 1 ~ 5 - n]、受信装置 [2]）を検証することができる。受信者は、第 1 電子データが送信された経路をオフラインで確認することができる。この受信装置 [2] は、 n 個の装置 [5 - 1 ~ 5 - n] と通信してログを収集することなく、第 1 電子データが送信された経路をオフラインで確認することができる。このため、 n 個の装置 [5 - 1 ~ 5 - n] は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、受信装置 [2] によって経路を把握するため、ハッカーの防止になる。

【0012】

本発明の電子データ送受信システムにおいて、第 1 装置 [5 - 1] は、送信装置 [1] から送信者認証子を受信した時刻を表す第 1 タイムスタンプに第 1 装置 [5 - 1] の署名を更に付与した第 2 電子データを生成する。第 n 装置 [5 - n] は、受信装置 [2] から受信者認証子を受信した時刻を表す第 2 タイムスタンプに第 n 装置 [5 - n] の署名を更に付与した第 $(n + 1)$ 電子データを生成する。受信装置 [2] は、第 $(n + 1)$ 電子データに付与された第 n 装置 [5 - n] の署名を除いた第 n 電子データと受信者認証子と第 2 タイムスタンプとを取出す。受信装置 [2] は、第 2 電子データに付与された第 1 装置 [5 - 1] の署名

を除いた第1電子データと受信者認証子と第1タイムスタンプとを取出す。

【0013】

本発明の電子データ送受信システムにおいて、第 n 装置[5-n]は、第 n 電子データと受信者認証子とに第 n 装置[5-n]の署名を付与した電子データである受信証拠データを生成して送信装置[1]に送信する。

【0014】

本発明の電子データ送受信システムにおいて、送信装置[1]は、 n 個の装置[5-1~5-n]の署名と受信者認証子とが格納された送信装置用データベース[18]を備えている。送信装置[1]は、第 n 装置[5-n]からの受信証拠データにより、受信装置[2]が第1電子データを受信したことを検証する。送信装置[1]は、受信証拠データに付与された第 n 装置[5-n]の署名を除いた第 n 電子データと受信者認証子とを取出す。送信装置[1]は、受信証拠データ及び第2電子データ以外の第($j+1$)電子データに付与された署名を除いた第 j 電子データを取出す。送信装置[1]は、第2電子データに付与された第1装置[5-1]の署名を除いた第1電子データと送信者認証子とを取出す。送信装置[1]は、送信装置用データベース[18]を参照して、第1電子データが受信装置[2]に送信されたことを認識する。

このように、本発明の電子データ送受信システムによれば、送信装置[1]が受信証拠データ、第 n 電子データ、…、第2電子データ、第1電子データの順で正しく確認(検証)できた場合、第1電子データは、受信装置[2]によって受信されたことが保証される。本発明の電子データ送受信システムによれば、送信装置[1]は、署名の履歴として第1電子データが受信装置[2]に送信された経路(送信装置[1]、 n 個の装置[5-1~5-n]、受信装置[2])を検証することができる。送信者は、第1電子データが送信されてきた経路をオフラインで確認することができる。この送信装置[1]は、 n 個の装置[5-1~5-n]と通信してログを収集することなく、第1電子データが送信されてきた経路をオフラインで確認することができる。このため、 n 個の装置[5-1~5-n]は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、送信装置[1]によって経路を把握す

るため、ハッカーの防止になる。

【0015】

本発明の電子データ送受信システムは、更に、第1電子データ記憶装置 [3 / 18] を具備する。第1電子データ記憶装置 [3 / 18] は、上記の送信装置用記憶装置 [3]、又は、上記の受信装置用データベース [18] である。送信装置 [1] は、第1電子データを送信する前に、第1電子データ記憶装置 [3 / 18] に第1電子データを格納している。送信装置 [1] は、第1電子データを取り出したとき、第1電子データ記憶装置 [3 / 18] を参照して、第1電子データが改ざんされることなく受信装置 [2] に送信されたことを認識する。

また、本発明の電子データ送受信システムによれば、送信装置 [1] は、取出した第1電子データと第1電子データ記憶装置 [3 / 18] に格納されている第1電子データとを比較することで第1電子データの改ざんを検出できる。

【0016】

本発明の電子データ送受信システムにおいて、第n装置 [5 - n] は、第n電子データと受信者認証子とに第n装置 [5 - n] の署名を付与した電子データである受信証拠データを生成し、受信証拠データから第1電子データを削除した受信証拠データを送信装置 [1] に送信する。送信装置 [1] は、第n装置 [5 - n] からの第1電子データが削除された受信証拠データに、第1電子データ記憶装置 [3 / 18] に格納された第1電子データを付加して受信証拠データを復元する。

【0017】

本発明の電子データ送受信システムにおいて、第1装置 [5 - 1] は、送信装置 [1] から送信者認証子を受信した時刻を表す第1タイムスタンプに第1装置 [5 - 1] の署名を更に付与した第2電子データを生成する。第n装置 [5 - n] は、受信装置 [2] から受信者認証子を受信した時刻を表す第2タイムスタンプに第n装置 [5 - n] の署名を更に付与した受信証拠データを生成する。送信装置 [1] は、受信証拠データに付与された第n装置 [5 - n] の署名を除いた第n電子データと受信者認証子と第2タイムスタンプとを取出す。送信装置 [1] は、第2電子データに付与された第1装置 [5 - 1] の署名を除いた第1電子

データと受信者認証子と第1タイムスタンプとを取出す。

【0018】

【発明の実施の形態】

添付図面を参照して、本発明による電子データ送受信システムの実施の形態を以下に説明する。

【0019】

図1は、本発明の電子データ送受信システムの構成を示す。本発明の電子データ送受信システムは、送受信装置1、2と、記憶装置3と、記憶装置4と、第1番目から第n番目（nは2以上の整数）までのn個の装置5-1～5-nとを具備する。送受信装置1、2と第1装置5-1、第2装置5-2、第3装置5-3、第4装置5-4、…、第n装置5-nとはネットワーク100に接続されている。送受信装置1には、送受信装置1用の記憶装置として記憶装置3が接続されている。送受信装置2には、送受信装置2用の記憶装置として記憶装置4が接続されている。

【0020】

この本発明の電子データ送受信システムは、送受信装置1が送信した電子データを送受信装置2が受信するまで保証するものである。図2は、本発明の電子データ送受信システムの概念を示す。ここで、本発明の電子データ送受信システムを具体的に説明するために、nを5とし、第1装置5-1を受付機器5-1とし、第2装置5-2を中継機器5-2とし、第3装置5-3を中継機器5-3とし、第4装置5-4を中継機器5-4とし、第n装置5-nを受付機器5-5とする。送受信装置1は、電子データを送受信装置2に送信するものとする。電子データは、送受信装置1から出力されて受付機器5-1、中継機器5-2、中継機器5-3、中継機器5-4、受付機器5-5を介して送受信装置2に出力される。

【0021】

電子データとしては、業者同士の業務に関する文書が記載された電子メールが例示され、その電子メールには画像が添付されている場合もある。また、電子データとしては、その業者同士の業務に関する電子データの他に、金融に関する電

子データ、民政に関する電子データが例示される。ここで、電子データは文書が記載された電子データ（電子メール）とし、以下、その電子データを電子文書と称する。

【0022】

図3は、送受信装置1、2の構成を示す。送受信装置1、2は、パーソナルコンピュータ、ワークステーション等で例示される情報処理装置である。送受信装置1、2は、コンピュータプログラムである送信部11、受信部12、署名部13、署名検証部14、電子文書検証部15、電子文書作成部16、登録部17を備え、データベース18を有する。送受信装置1、2には、利用者の操作により電子文書作成部16が電子文書を作成するための入力装置（図示しない）が接続されている。送受信装置1、2の署名部13は、公開鍵基盤を利用して秘密鍵で電子文書に送受信装置1、2の署名を行うものである。送受信装置1のデータベース18には、受付機器5-1、5-5の署名、中継機器5-2、5-3、5-4の署名、送受信装置2の署名（後述の認証子）がそれぞれ公開鍵証明書として格納されている。送受信装置2のデータベース18には、送受信装置1の署名（後述の認証子）、受付機器5-1、5-5の署名、中継機器5-2、5-3、5-4の署名がそれぞれ公開鍵証明書として格納されている。

【0023】

図4は、受付機器5-1、5-5の構成を示す。受付機器5-1、5-5は、ワークステーション、サーバ等で例示される情報処理装置である。受付機器5-1、5-5は、コンピュータプログラムである送信部21、受信部22、署名部23、署名検証部24、証拠データ生成部25、タイムスタンプ生成部26、保存制御部27を備え、データベース28を有する。受付機器5-1のデータベース28には、送受信装置1、2の署名（後述の認証子）、中継機器5-2、5-3、5-4の署名、受付機器5-5の署名がそれぞれ公開鍵証明書として格納されている。受付機器5-5のデータベース28には、送受信装置1、2の署名（後述の認証子）、受付機器5-1の署名、中継機器5-2、5-3、5-4の署名がそれぞれ公開鍵証明書として格納されている。また、受付機器5-1、5-5の署名検証部24は、送受信装置1、2のアドレスを予め認識している。な

お、受付機器 5-1、5-5 をなくして、受付機器 5-1、5-5 の機能（送信部 21、受信部 22、証拠データ生成部 25、タイムスタンプ生成部 26、署名部 23、署名検証部 24、保存制御部 27、データベース 28）をアプリケーションとして送受信装置 1、2 に実装することも可能である。

【0024】

図 5 は、中継機器 5-2、5-3、5-4 の構成を示す。中継機器 5-2、5-3、5-4 は、コンピュータプログラムである送信部 31、受信部 32、署名部 33、署名検証部 34 を備え、データベース 38 を有する。中継機器 5-2 のデータベース 38 には、受付機器 5-1、5-5、中継機器 5-3、5-4 の署名がそれぞれ公開鍵証明書として格納されている。中継機器 5-3 のデータベース 38 には、受付機器 5-1、5-5、中継機器 5-2、5-4 の署名がそれぞれ公開鍵証明書として格納されている。中継機器 5-4 のデータベース 38 には、受付機器 5-1、5-5、中継機器 5-2、5-3 の署名がそれぞれ公開鍵証明書として格納されている。本実施例では中継機器を 3 つとしている。しかし受付機器 5-1、5-5 同士が直接通信できる環境では中継機器 5-2、5-3、5-4 は必要ない。また電子文書の処理手続きのプロセスなどが長いときには中継機器が複数台存在する。

【0025】

記憶装置 3、記憶装置 4 は、フレキシブルディスク、ハードディスク、データベース、ファイルサーバ等で例示される装置である。記憶装置 3、記憶装置 4 には、電子文書等で例示されるデータ（後述）が送受信装置 1、2 によって格納される。

【0026】

次に、本発明の電子データ送受信システムの動作について説明する。

送受信装置 1 から出力される第 1 電子文書は、受付機器 5-1、中継機器 5-2、中継機器 5-3、中継機器 5-4、受付機器 5-5 を介して送受信装置 2 に出力される。このため、本発明の電子データ送受信システムの動作の説明では、送受信装置 1 を送信装置 1 とし、送受信装置 2 を受信装置 2 とする。

【0027】

まず、第1電子文書の送受信の証拠となる署名データ（署名、送信認証子、送信証拠データ、受信認証子、受信証拠データ）の生成について説明する。

【0028】

図6に示されるように、送信装置1を利用する送信者は、受信装置2に送る第1電子文書を作成するために、送信装置1の入力装置を操作する。送信装置1の電子文書作成部16は、その入力装置の操作に応じて、第1電子文書を作成する（ステップA1）。

送信者が送信装置1の入力装置を操作して第1電子文書を受信装置2に送るとき、送信装置1の送信部11は、その入力装置の操作に応じて、第1電子文書の送信要求を受付機器5-1に送信する（ステップA2）。

【0029】

受付機器5-1の受信部22は、送信装置1からの第1電子文書の送信要求を受信する。その受信部22が第1電子文書の送信要求を受信したとき、受付機器5-1の署名部23は、ランダムな文字列を生成する。受付機器5-1の送信部21は、そのランダムな文字列を送信装置1に送信する（ステップA3）。

【0030】

送信装置1の受信部12は、受付機器5-1からのランダムな文字列を受信する。送信装置1の署名部13は、その受信部12が受信したランダムな文字列に送信装置1の秘密鍵で署名して、第1電子文書の送信を認証する送信者認証子を生成する（ステップA4）。

送信装置1の登録部17は、送信装置1の送信部11が第1電子文書を送信する前に、記憶装置3又は送信装置1のデータベース18に第1電子文書を保管用電子文書として格納しておく（ステップA5）。ここで、この保管用電子文書は記憶装置3に格納されるものとする。

送信装置1の送信部11は、第1電子文書と送信者認証子とを受付機器5-1に送信する（ステップA6）。ここで、第1電子文書は、第1電子文書を受信装置2宛てに送るためのアドレス（受信装置2のアドレス）を含む。

【0031】

受付機器5-1の受信部22は、送信装置1からの第1電子文書と送信者認証

子とを受信する。その受信部 22 が第 1 電子文書と送信者認証子とを受信したとき、受付機器 5-1 のタイムスタンプ生成部 26 は、送信装置 1 から送信者認証子を受信した時刻を表す第 1 タイムスタンプを生成する（ステップ A 7）。

このとき、受付機器 5-1 の署名検証部 24 は、受付機器 5-1 のデータベース 28 を参照して、送信者認証子と送信装置 1 の公開鍵証明書とを照合し、送信者認証子が送信装置 1 の公開鍵証明書と一致するか否かを検証する（ステップ A 8）。

【0032】

検証の結果、一致する場合、受付機器 5-1 の証拠データ生成部 25 は、第 1 電子文書に送信者認証子、第 1 タイムスタンプを加えてハッシュ値を生成する。受付機器 5-1 の証拠データ生成部 25 は、そのハッシュ値に受付機器 5-1 の秘密鍵で署名することにより、第 1 電子文書と送信者認証子と第 1 タイムスタンプとに受付機器 5-1 の署名を付与した電子データである送信証拠データを生成する（ステップ A 9）。送信証拠データを生成する場合、第 1 タイムスタンプは省略してもよい。受付機器 5-1 の送信部 21 は、送信証拠データを送信装置 1 に送信する（ステップ A 10）。

また、検証の結果、一致しない場合、受付機器 5-1 の送信部 21 は、一致しない旨を表す情報を送信装置 1 に送信する。送信装置 1 は、その情報に応じて、再度、第 1 電子文書と送信者認証子とを受付機器 5-1 に送信し、受付機器 5-1 は、再度、送信者認証子を検証しても一致しない場合、第 1 電子文書を送信できない旨を表す情報を送信装置 1 に送信する（このステップは図示しない）。

【0033】

送信装置 1 の受信部 12 は、受付機器 5-1 からの送信証拠データを受信する。その受信部 12 が送信証拠データを受信したとき、送信装置 1 の署名検証部 14 は、送信装置 1 のデータベース 18 を参照して、送信証拠データの署名と受付機器 5-1 の公開鍵証明書とを照合し、送信証拠データの署名が受付機器 5-1 の公開鍵証明書と一致するか否かを検証する（ステップ A 11）。

検証の結果、一致する場合、送信装置 1 の登録部 17 は、送信証拠データを記憶装置 3 に格納する（ステップ A 12）。本発明の電子データ送受信システムに

よれば、受付機器 5-1 の署名を付与した送信証拠データを記憶装置 3 に格納するため、送信装置 1 を用いて第 1 電子文書を送信した送信者が第 1 電子文書を送信していないと否認（送信拒否）することができない。

また、検証の結果、一致しない場合、送信装置 1 は、再度、第 1 電子文書と送信者認証子とを送信し、受付機器 5-1 は、再度、送信者認証子を検証しても一致しない場合、第 1 電子文書を送信できない旨を表す情報を送信装置 1 に送信する（このステップは図示しない）。

【0034】

受付機器 5-1 の署名部 23 は、第 1 電子文書に送信者認証子、第 1 タイムスタンプを加えてハッシュ値を生成する。受付機器 5-1 の証拠データ生成部 25 は、そのハッシュ値に受付機器 5-1 の秘密鍵で署名することにより、第 1 電子文書と送信者認証子と第 1 タイムスタンプとに受付機器 5-1 の署名を付与した第 2 電子文書を生成する（ステップ A13、図 9 参照）。第 2 電子文書を生成する場合、第 1 タイムスタンプは省略してもよい。

受付機器 5-1 の送信部 21 は、第 2 電子文書の中継機器 5-2 に送信する（ステップ A14）。第 2 電子文書は、受信装置 2 のアドレスを含む。

【0035】

図 7 に示されるように、中継機器 5-2 の受信部 32 は、受付機器 5-1 からの第 2 電子文書を受信する。その受信部 32 が第 2 電子文書を受信したとき、中継機器 5-2 の署名検証部 34 は、中継機器 5-2 のデータベース 38 を参照して、第 2 電子文書の署名と受付機器 5-1 の公開鍵証明書とを照合し、第 2 電子文書の署名が受付機器 5-1 の公開鍵証明書と一致するか否かを検証する（ステップ A15）。その署名検証部 34 は、検証することにより、中継してよいかどうかの正当性確認をする。ただし受付機器 5-1 と中継機器 5-2 の間に信頼関係が成立する場合は署名検証を省略してもよい。

【0036】

検証の結果、一致する場合、中継機器 5-2 の署名部 33 は、第 2 電子文書に中継機器 5-2 の秘密鍵で署名することによって、第 2 電子文書に中継機器 5-2 の署名を付与した第 3 電子文書を生成する（ステップ A16、図 9 参照）。中

継機器 5 - 2 の送信部 3 1 は、第 3 電子文書の中継機器 5 - 3 に送信する（ステップ A 1 7）。第 3 電子文書は、受信装置 2 のアドレスを含む。

また、検証の結果、一致しない場合、中継機器 5 - 2 の送信部 3 1 は、一致しない旨を表す情報を受付機器 5 - 1 に送信する。受付機器 5 - 1 は、その情報に応じて、再度、第 2 電子文書の中継機器 5 - 2 に送信し、中継機器 5 - 2 は、再度、第 2 電子文書を検証しても一致しない場合、第 2 電子文書（第 1 電子文書）を送信できない旨を表す情報を送信装置 1 に送信する（このステップは図示しない）。

【 0 0 3 7 】

中継機器 5 - 3 の受信部 3 2 は、中継機器 5 - 2 からの第 3 電子文書を受信する。その受信部 3 2 が第 3 電子文書を受信したとき、中継機器 5 - 3 の署名検証部 3 4 は、中継機器 5 - 3 のデータベース 3 8 を参照して、第 3 電子文書の署名と中継機器 5 - 2 の公開鍵証明書とを照合し、第 3 電子文書の署名が中継機器 5 - 2 の公開鍵証明書と一致するか否かを検証する（ステップ A 1 8）。その署名検証部 3 4 は、検証することにより、中継してよいかどうかの正当性確認をする。ただし受付機器 5 - 2 と中継機器 5 - 3 の間に信頼関係が成立する場合は署名検証を省略してもよい。

【 0 0 3 8 】

検証の結果、一致する場合、中継機器 5 - 3 の署名部 3 3 は、第 3 電子文書に中継機器 5 - 3 の秘密鍵で署名することによって、第 3 電子文書に中継機器 5 - 3 の署名を付与した第 4 電子文書を生成する（ステップ A 1 9、図 9 参照）。中継機器 5 - 3 の送信部 3 1 は、第 4 電子文書の中継機器 5 - 4 に送信する（ステップ A 2 0）。第 4 電子文書は、受信装置 2 のアドレスを含む。

また、検証の結果、一致しない場合、中継機器 5 - 3 の送信部 3 1 は、一致しない旨を表す情報を中継機器 5 - 2 に送信する。中継機器 5 - 2 は、その情報に応じて、再度、第 3 電子文書の中継機器 5 - 3 に送信し、中継機器 5 - 3 は、再度、第 3 電子文書を検証しても一致しない場合、第 3 電子文書（第 1 電子文書）を送信できない旨を表す情報を送信装置 1 に送信する（このステップは図示しない）。

【0 0 3 9】

中継機器 5 - 4 の受信部 3 2 は、中継機器 5 - 3 からの第 4 電子文書を受信する。その受信部 3 2 が第 4 電子文書を受信したとき、中継機器 5 - 4 の署名検証部 3 4 は、中継機器 5 - 4 のデータベース 3 8 を参照して、第 4 電子文書の署名と中継機器 5 - 3 の公開鍵証明書とを照合し、第 4 電子文書の署名が中継機器 5 - 3 の公開鍵証明書と一致するか否かを検証する（ステップ A 2 1）。その署名検証部 3 4 は、検証することにより、中継してよいかどうかの正当性確認をする。ただし受付機器 5 - 3 と中継機器 5 - 4 の間に信頼関係が成立する場合は署名検証を省略してもよい。

【0 0 4 0】

検証の結果、一致する場合、中継機器 5 - 4 の署名部 3 3 は、第 4 電子文書に中継機器 5 - 4 の秘密鍵で署名することによって、第 4 電子文書に中継機器 5 - 4 の署名を付与した第 5 電子文書を生成する（ステップ A 2 2、図 9 参照）。中継機器 5 - 4 の送信部 3 1 は、第 5 電子文書を受付機器 5 - 5 に送信する（ステップ A 2 3）。第 5 電子文書は、受信装置 2 のアドレスを含む。

また、検証の結果、一致しない場合、中継機器 5 - 4 の送信部 3 1 は、一致しない旨を表す情報を中継機器 5 - 3 に送信する。中継機器 5 - 3 は、その情報に応じて、再度、第 4 電子文書の中継機器 5 - 4 に送信し、中継機器 5 - 4 は、再度、第 4 電子文書を検証しても一致しない場合、第 4 電子文書（第 1 電子文書）を送信できない旨を表す情報を送信装置 1 に送信する（このステップは図示しない）。

【0 0 4 1】

図 8 に示されるように、受付機器 5 - 5 の受信部 2 2 は、中継機器 5 - 4 からの第 5 電子文書を受信する。その受信部 2 2 が第 5 電子文書を受信したとき、受付機器 5 - 5 の署名検証部 2 4 は、受付機器 5 - 5 のデータベース 2 8 を参照して、第 5 電子文書の署名と中継機器 5 - 4 の公開鍵証明書とを照合し、第 5 電子文書の署名が中継機器 5 - 4 の公開鍵証明書と一致するか否かを検証する。その署名検証部 2 4 は、受付機器 5 - 5 のデータベース 2 8 を参照して、第 5 電子文書に含まれるアドレスにより受信装置 2 宛ての電子文書であるか否か確認する（

ステップA24)。

【0042】

検証と確認の結果、一致する場合、受付機器5-5の送信部21は、第5電子文書を受信したことを表す受信通知を受信装置2に送信する(ステップA25)

。

また、検証の結果、一致しない場合、受付機器5-5の送信部21は、一致しない旨を表す情報を中継機器5-4に送信する。中継機器5-4は、その情報に応じて、再度、第5電子文書を受付機器5-5に送信し、受付機器5-5は、再度、第5電子文書を検証しても一致しない場合、第5電子文書(第1電子文書)を送信できない旨を表す情報を送信装置1に送信する(このステップは図示しない)。

【0043】

受信装置2の受信部12は、受付機器5-5からの受信通知を受信する。その受信部12が受信通知を受信したとき、受信装置2の送信部11は、第5電子文書の受信要求を受付機器5-5に送信する(ステップA26)。

【0044】

受付機器5-5の受信部22は、受信装置2からの第5電子文書の受信要求を受信する。その受信部22が第5電子文書の受信要求を受信したとき、受付機器5-5の署名部23は、ランダムな文字列を生成する。受付機器5-5の送信部21は、そのランダムな文字列を受信装置2に送信する(ステップA27)。

【0045】

受信装置2の受信部12は、受付機器5-5からのランダムな文字列を受信する。受信装置2の署名部13は、その受信部12が受信したランダムな文字列に受信装置2の秘密鍵で署名して、第5電子文書の受信を認証する受信者認証子を生成する(ステップA28)。

受信装置2の送信部11は、受信者認証子を受付機器5-5に送信する(ステップA29)。

【0046】

受付機器5-5の受信部22は、受信装置2からの受信者認証子を受信する。

その受信部 22 が受信者認証子を受信したとき、受付機器 5-5 のタイムスタンプ生成部 26 は、受信装置 2 から受信者認証子を受信した時刻を表す第 2 タイムスタンプを生成する（ステップ A30）。

このとき、受付機器 5-5 の署名検証部 24 は、受付機器 5-5 のデータベース 28 を参照して、受信者認証子と受信装置 2 の公開鍵証明書とを照合し、受信者認証子が受信装置 2 の公開鍵証明書と一致するか否かを検証する（ステップ A31）。

【0047】

検証の結果、一致する場合、受付機器 5-5 の署名部 23 は、第 5 電子文書に受信者認証子、第 2 タイムスタンプを加えてハッシュ値を生成する。受付機器 5-5 の署名部 23 は、そのハッシュ値に受付機器 5-5 の秘密鍵で署名することにより、第 5 電子文書と受信者認証子と第 2 タイムスタンプとに受付機器 5-5 の署名を付与した第 6 電子文書を生成する（ステップ A32、図 9 参照）。第 6 電子文書を生成する場合、第 2 タイムスタンプは省略してもよい。受付機器 5-5 の送信部 21 は、第 6 電子文書を受信装置 2 に送信する（ステップ A33）。

また、検証の結果、一致しない場合、受付機器 5-5 の送信部 21 は、一致しない旨を表す情報を受信装置 2 に送信する。受信装置 2 は、その情報に応じて、再度、受信者認証子を受付機器 5-5 に送信し、受付機器 5-5 は、再度、受信者認証子を検証しても一致しない場合、第 5 電子文書（第 1 電子文書）を送信できない旨を表す情報を送信装置 1 に送信する（このステップは図示しない）。

【0048】

受信装置 2 の受信部 12 は、受付機器 5-5 からの第 6 電子文書を受信する。その受信部 12 が第 6 電子文書を受信したとき、受信装置 2 の署名検証部 14 は、受信装置 2 のデータベース 18 を参照して、第 6 電子文書の署名と受付機器 5-5 の公開鍵証明書とを照合し、第 6 電子文書の署名が受付機器 5-5 の公開鍵証明書と一致するか否かを検証する（ステップ A34）。

検証の結果、一致する場合、受信装置 2 の登録部 17 は、第 6 電子文書を記憶装置 4 に格納する（ステップ A35）。第 6 電子文書は、送信者認証子と、署名（受付機器 5-1、中継器 5-2、中継器 5-3、中継器 5-4、受付機器 5-

5) と、受信者認証子とが付与された第1電子文書である。本発明の電子データ送受信システムによれば、第6電子文書を記憶装置4に格納するため、受信装置2を利用する受信者が第1電子文書を受取っていないと否認（受信拒否）することができない。

また、検証の結果、一致しない場合、受信装置2の送信部11は、一致しない旨を表す情報を受付機器5-5に送信する。受付機器5-5は、その情報に応じて、再度、第6電子文書を受信装置2に送信し、受信装置2は、再度、第6電子文書を検証しても一致しない場合、第6電子文書（第1電子文書）を送信できない旨を表す情報を送信装置1に送信する（このステップは図示しない）。

【0049】

受付機器5-5の証拠データ生成部25は、第5電子文書に受信者認証子、第2タイムスタンプを加えてハッシュ値を生成する。受付機器5-5の証拠データ生成部25は、そのハッシュ値に受付機器5-5の秘密鍵で署名することにより、第5電子文書と受信者認証子と第2タイムスタンプとに受付機器5-5の署名を付与した電子データである受信証拠データを生成する（ステップA36、図10参照）。受信証拠データを生成する場合、第2タイムスタンプは省略してもよい。

受付機器5-5の送信部21は、受信証拠データを送信装置1に送信する（ステップA37）。受信証拠データは、受付機器5-5から中継機器5-4、中継機器5-3、中継機器5-2、受付機器5-1を介して送信装置1に送信される。または、受信証拠データは、受付機器5-5から直接、送信装置1に送信される。

【0050】

送信装置1の受信部12は、受付機器5-5からの受信証拠データを受信する。その受信部12が受信証拠データを受信したとき、送信装置1の署名検証部14は、送信装置1のデータベース18を参照して、受信証拠データの署名と受付機器5-5の公開鍵証明書とを照合し、受信証拠データの署名が受付機器5-5の公開鍵証明書と一致するか否かを検証する（ステップA38）。

【0051】

検証の結果、一致する場合、送信装置 1 の登録部 1 7 は、受信証拠データを記憶装置 3 に格納する（ステップ A 3 9）。

また、検証の結果、一致しない場合、受信装置 2 の送信部 1 1 は、一致しない旨を表す情報を受付機器 5 - 5 に送信する。受付機器 5 - 5 は、その情報に応じて、再度、受信証拠データを受信装置 2 に送信し、受信装置 2 は、再度、受信証拠データを検証しても一致しない場合、第 6 電子文書（第 1 電子文書）を受信しても受け付けない旨を表す情報を送信装置 1 に送信する（このステップは図示しない）。

【 0 0 5 2 】

本発明の電子データ送受信システムによれば、送信者認証子と、第 6 電子文書が生成されるまでに付与された署名（受付機器 5 - 1、中継器 5 - 2、中継器 5 - 3、中継器 5 - 4、受付機器 5 - 5）と、受信者認証子とにより、送信装置 1 を用いて第 1 電子文書を送信した送信者が第 1 電子文書を送信していないと否認（送信拒否）することができない。また、本発明の電子データ送受信システムによれば、受信装置 2 を利用する受信者が第 1 電子文書を受取っていないと否認（受信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置 1 が送信した第 1 電子文書を受信装置 2 が受信するまで保証する。

【 0 0 5 3 】

次に、受信装置 2 が行う第 6 電子文書の検証について説明する。

【 0 0 5 4 】

図 1 1 に示されるように、受信装置 2 の電子文書検証部 1 5 は、受信装置 2 のデータベース 1 8 を参照して、記憶装置 4 に格納された第 6 電子文書の署名と受付機器 5 - 5 の公開鍵証明書とを照合し、第 6 電子文書の署名が受付機器 5 - 5 の公開鍵証明書と一致するか否かを検証する（ステップ B 1）。

検証の結果、受信装置 2 の電子文書検証部 1 5 は、一致する第 6 電子文書に付与された受付機器 5 - 5 の署名を除いた第 5 電子文書と受信者認証子と第 2 タイムスタンプとを取出す（ステップ B 2、図 9 参照）。

【 0 0 5 5 】

受信装置 2 の電子文書検証部 1 5 は、受信装置 2 のデータベース 1 8 を参照して、第 5 電子文書の署名と中継機器 5 - 4 の公開鍵証明書とを照合し、第 5 電子文書の署名が中継機器 5 - 4 の公開鍵証明書と一致するか否かを検証する（ステップ B 3）。

検証の結果、受信装置 2 の電子文書検証部 1 5 は、一致する第 5 電子文書に付与された中継機器 5 - 4 の署名を除いた第 4 電子文書を取り出す（ステップ B 4、図 9 参照）。

【 0 0 5 6 】

受信装置 2 の電子文書検証部 1 5 は、受信装置 2 のデータベース 1 8 を参照して、第 4 電子文書の署名と中継機器 5 - 3 の公開鍵証明書とを照合し、第 4 電子文書の署名が中継機器 5 - 3 の公開鍵証明書と一致するか否かを検証する（ステップ B 5）。

検証の結果、一致するため、受信装置 2 の電子文書検証部 1 5 は、第 4 電子文書に付与された中継機器 5 - 3 の署名を除いた第 3 電子文書を取り出す（ステップ B 6、図 9 参照）。

【 0 0 5 7 】

受信装置 2 の電子文書検証部 1 5 は、受信装置 2 のデータベース 1 8 を参照して、第 3 電子文書の署名と中継機器 5 - 2 の公開鍵証明書とを照合し、第 3 電子文書の署名が中継機器 5 - 2 の公開鍵証明書と一致するか否かを検証する（ステップ B 7）。

検証の結果、一致するため、受信装置 2 の電子文書検証部 1 5 は、第 3 電子文書に付与された中継機器 5 - 2 の署名を除いた第 2 電子文書を取り出す（ステップ B 8、図 9 参照）。

【 0 0 5 8 】

受信装置 2 の電子文書検証部 1 5 は、受信装置 2 のデータベース 1 8 を参照して、第 2 電子文書の署名と受付機器 5 - 1 の公開鍵証明書とを照合し、第 2 電子文書の署名が受付機器 5 - 1 の公開鍵証明書と一致するか否かを検証する（ステップ B 9）。

検証の結果、一致するため、受信装置 2 の電子文書検証部 1 5 は、第 2 電子文

書に付与された受付機器 5-1 の署名を除いた第 1 電子文書と送信者認証子と第 1 タイムスタンプとを取出す（ステップ B 10、図 9 参照）。

【0059】

受信装置 2 の電子文書検証部 15 は、受信装置 2 のデータベース 18 を参照して、送信者認証子と送信装置 1 の公開鍵証明書とを照合し、送信者認証子が送信装置 1 の公開鍵証明書と一致するか否かを検証する（ステップ B 11）。

検証の結果、一致するため、受信装置 2 の電子文書検証部 15 は、送信装置 1 が第 1 電子文書を送信したことを認識する（ステップ B 12）。

【0060】

このように、本発明の電子データ送受信システムによれば、受信装置 2 が第 6 電子文書、第 5 電子文書、第 4 電子文書、第 3 電子文書、第 2 電子文書、第 1 電子文書の順で正しく確認（検証）できた場合、第 1 電子文書は、送信装置 1 によって送信されたことが保証される。また、本発明の電子データ送受信システムによれば、受信装置 2 は、署名の履歴として第 1 電子文書が受信装置 2 に送信された経路（送信装置 1、受付機器 5-1、中継器 5-2、中継器 5-3、中継器 5-4、受付機器 5-5、受信装置 2）を検証することができる。受信者は、その経路をオフラインで確認することができる。この受信装置 2 は、受付機器 5-1、中継器 5-2、中継器 5-3、中継器 5-4、受付機器 5-5 と通信してログを収集することなく、第 1 電子文書が送信された経路をオフラインで確認することができる。このため、受付機器 5-1、中継器 5-2、中継器 5-3、中継器 5-4、受付機器 5-5 は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、受信装置 2 によって経路を把握するため、ハッカーを防止する。

【0061】

次に、送信装置 1 が行う受信証拠データの検証について説明する。

【0062】

図 12 に示されるように、送信装置 1 の電子文書検証部 15 は、送信装置 1 のデータベース 18 を参照して、記憶装置 3 に格納された受信証拠データの署名と受付機器 5-5 の公開鍵証明書とを照合し、受信証拠データの署名が受付機器 5

ー 5 の公開鍵証明書と一致するか否かを検証する（ステップ C 1）。

検証の結果、一致するため、送信装置 1 の電子文書検証部 15 は、受信証拠データに付与された受付機器 5-5 の署名を除いた第 5 電子文書と受信者認証子と第 2 タイムスタンプとを取出す（ステップ C 2、図 10 参照）。

【0063】

送信装置 1 の電子文書検証部 15 は、送信装置 1 のデータベース 18 を参照して、受信者認証子と受信装置 2 の公開鍵証明書とを照合し、受信者認証子が送信装置 1 の公開鍵証明書と一致するか否かを検証する（ステップ C 3）。

検証の結果、一致するため、送信装置 1 の電子文書検証部 15 は、送信装置 1 のデータベース 18 を参照して、第 5 電子文書の署名と中継機器 5-4 の公開鍵証明書とを照合し、第 5 電子文書の署名が中継機器 5-4 の公開鍵証明書と一致するか否かを検証する（ステップ C 4）。

検証の結果、一致するため、送信装置 1 の電子文書検証部 15 は、第 5 電子文書に付与された中継機器 5-4 の署名を除いた第 4 電子文書を取出す（ステップ C 5、図 10 参照）。

【0064】

送信装置 1 の電子文書検証部 15 は、送信装置 1 のデータベース 18 を参照して、第 4 電子文書の署名と中継機器 5-3 の公開鍵証明書とを照合し、第 4 電子文書の署名が中継機器 5-3 の公開鍵証明書と一致するか否かを検証する（ステップ C 6）。

検証の結果、一致するため、送信装置 1 の電子文書検証部 15 は、第 4 電子文書に付与された中継機器 5-3 の署名を除いた第 3 電子文書を取出す（ステップ C 7、図 10 参照）。

【0065】

送信装置 1 の電子文書検証部 15 は、送信装置 1 のデータベース 18 を参照して、第 3 電子文書の署名と中継機器 5-2 の公開鍵証明書とを照合し、第 3 電子文書の署名が中継機器 5-2 の公開鍵証明書と一致するか否かを検証する（ステップ C 8）。

検証の結果、一致するため、送信装置 1 の電子文書検証部 15 は、第 3 電子文

書に付与された中継機器 5-2 の署名を除いた第 2 電子文書を取り出す（ステップ C9、図 10 参照）。

【0066】

送信装置 1 の電子文書検証部 15 は、送信装置 1 のデータベース 18 を参照して、第 2 電子文書の署名と受付機器 5-1 の公開鍵証明書とを照合し、第 2 電子文書の署名が受付機器 5-1 の公開鍵証明書と一致するか否かを検証する（ステップ C10）。

検証の結果、一致するため、送信装置 1 の電子文書検証部 15 は、第 2 電子文書に付与された受付機器 5-1 の署名を除いた第 1 電子文書と送信者認証子と第 1 タイムスタンプとを取り出す（ステップ C11、図 10 参照）。

【0067】

送信装置 1 の電子文書検証部 15 は、記憶装置 3 を参照して、いま取出した第 1 電子文書と記憶装置 3 に格納されている保管用電子文書（第 1 電子文書）とを照合し、取出した第 1 電子文書が保管用電子文書と一致するか否かを検証する（ステップ C12）。

検証の結果、一致するため、送信装置 1 の電子文書検証部 15 は、第 1 電子文書が改ざんされることなく受信装置 2 に送信されたことを認識する（ステップ C13）。

【0068】

このように、本発明の電子データ送受信システムによれば、送信装置 1 が受信証拠データ、第 5 電子文書、第 4 電子文書、第 3 電子文書、第 2 電子文書、第 1 電子文書の順で正しく確認（検証）できた場合、第 1 電子文書は、受信装置 2 によって受信されたことが保証される。また、本発明の電子データ送受信システムによれば、送信装置 1 は、取出した第 1 電子文書と記憶装置 3 に格納されている保管用電子文書（第 1 電子文書）とを比較することで第 1 電子文書の改ざんを検出できる。本発明の電子データ送受信システムによれば、送信装置 1 は、署名の履歴として第 1 電子文書が受信装置 2 に送信された経路（送信装置 1、受付機器 5-1、中継器 5-2、中継器 5-3、中継器 5-4、受付機器 5-5、受信装置 2）を検証することができる。送信者は、その経路をオフラインで確認するこ

とができる。この送信装置 1 は、受付機器 5-1、中継器 5-2、中継器 5-3、中継器 5-4、受付機器 5-5 と通信してログを収集することなく、第 1 電子文書が送信されてきた経路をオフラインで確認することができる。このため、受付機器 5-1、中継器 5-2、中継器 5-3、中継器 5-4、受付機器 5-5 は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、送信装置 1 によって経路を把握するため、ハッカーを防止する。

【0069】

上述のステップ A 36 にて受信証拠データを生成する場合、電子文書は省略してもよい（図 14 参照）。

【0070】

この場合、図 13 に示されるように、受付機器 5-5 の証拠データ生成部 25 は、ステップ A 36 にて受信証拠データを生成した後、その受信証拠データから第 1 電子データを削除する（ステップ A 40）。受付機器 5-5 の送信部 21 は、ステップ A 36 にて、第 1 電子データが削除された受信証拠データを送信装置 1 に送信する。

送信装置 1 の受信部 12 は、第 1 電子データが削除された受信証拠データを受付機器 5-5 から受信する。このとき、送信装置 1 の署名検証部 14 は、第 1 電子データが削除された受信証拠データに、記憶装置 3 に格納されている保管用電子文書（第 1 電子文書）を付加して受信証拠データを復元する（ステップ A 41）。その後、送信装置 1 は、ステップ A 38、A 39、C 1～C 13 を実行する。

【0071】

【発明の効果】

本発明の電子データ送受信システムによれば、送受信装置 1（送信装置 1）が送信した電子データ（第 1 電子文書）を送受信装置 2（受信装置 2）が受信するまで保証する。

また、本発明の電子データ送受信システムによれば、送受信装置 1（送信装置 1）、送受信装置 2（受信装置 2）は、電子データ（第 1 電子文書）が送受信装

置 2（受信装置 2）に送信された経路を検証することができる。

また、本発明の電子データ送受信システムによれば、送受信装置 1（送信装置 1）は、電子データ（第 1 電子文書）と記憶装置 3 に格納されている電子データ（第 1 電子文書）とを比較することで改ざんを検出できる。

また、本発明の電子データ送受信システムによれば、送受信装置 1（送信装置 1）、送受信装置 2（受信装置 2）によって経路を把握するため、ハッカーを防止する。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の電子データ送受信システムの構成を示す図である。

【図 2】

図 2 は、本発明の電子データ送受信システムの概念を示す図である。

【図 3】

図 3 は、本発明の電子データ送受信システムの送受信装置の構成を示す図である。

【図 4】

図 4 は、本発明の電子データ送受信システムの受付機器の構成を示す図である。

【図 5】

図 5 は、本発明の電子データ送受信システムの中継機器の構成を示す図である。

【図 6】

図 6 は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図 7】

図 7 は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図 8】

図 8 は、本発明の電子データ送受信システムの動作を示すフローチャートである。

る。

【図 9】

図 9 は、本発明の電子データ送受信システムにおける電子文書を説明するための図である。

【図 10】

図 10 は、本発明の電子データ送受信システムにおける電子文書を説明するための図である。

【図 11】

図 11 は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図 12】

図 12 は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図 13】

図 13 は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図 14】

図 14 は、本発明の電子データ送受信システムにおける電子文書を説明するための図である。

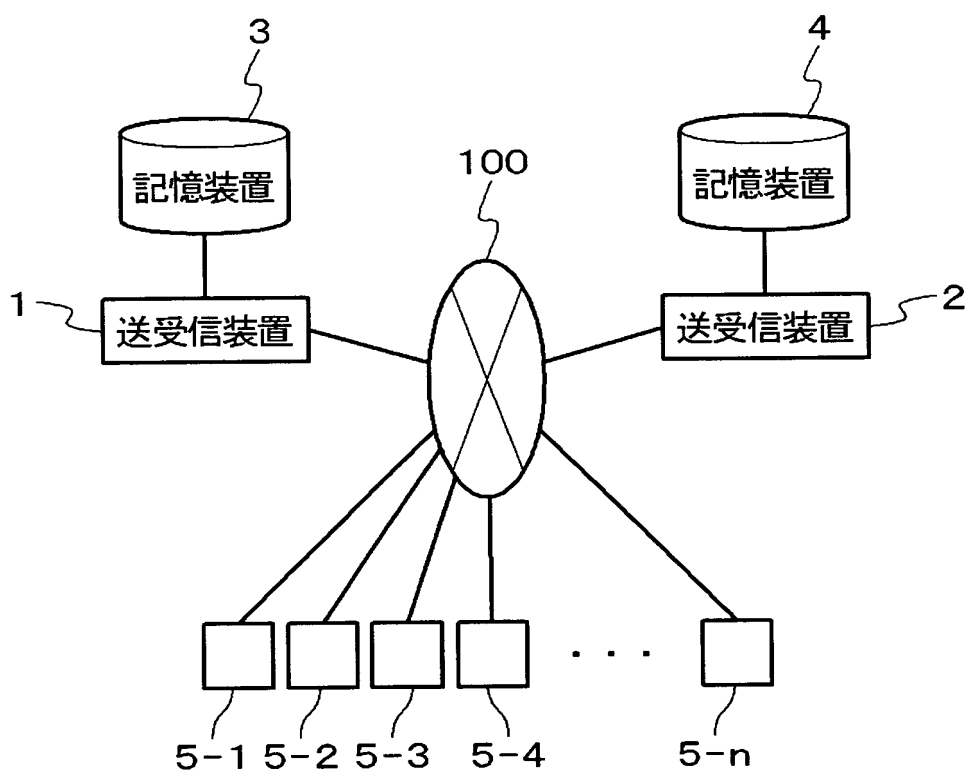
【符号の説明】

- 1 送受信装置（送信装置）
- 2 送受信装置（受信装置）
- 3、4 記憶装置
- 5-1、5-5 受付機器
- 5-2、5-3、5-4 中継機器
- 11、21、31 送信部
- 12、22、32 受信部
- 13、23、33 署名部
- 14、24、34 署名検証部

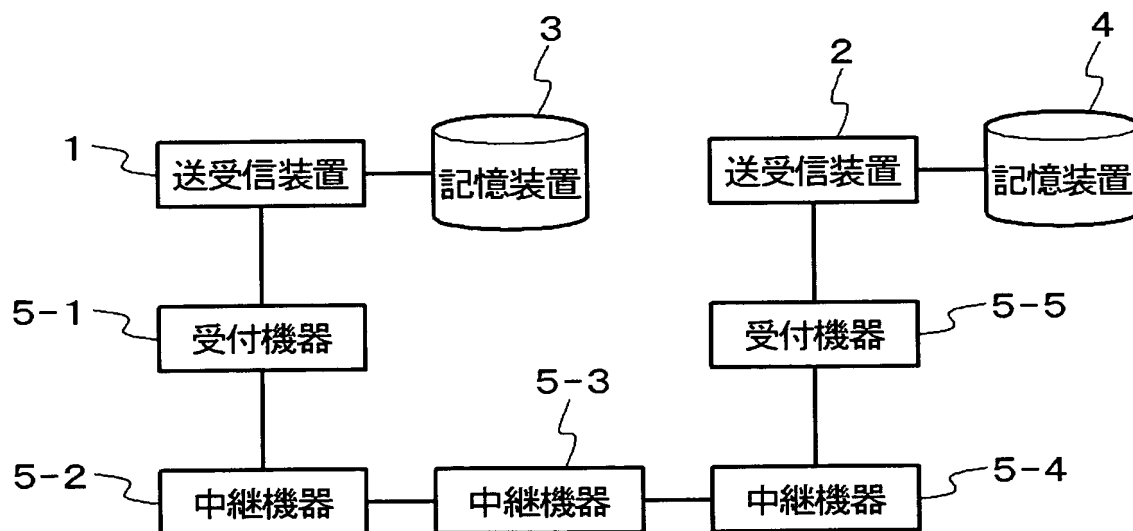
- 1 5 電子文書検証部
- 1 6 電子文書作成部
- 1 7 登録部
- 1 8、2 8、3 8 データベース
- 2 5 証拠データ生成部
- 2 6 タイムスタンプ生成部
- 2 7 保存制御部
- 1 0 0 ネットワーク

【書類名】 図面

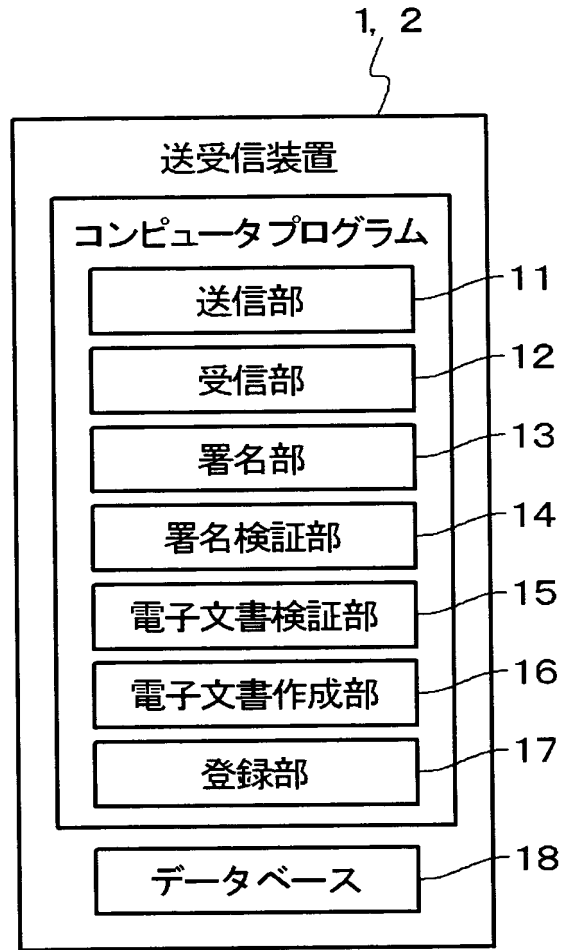
【図 1】



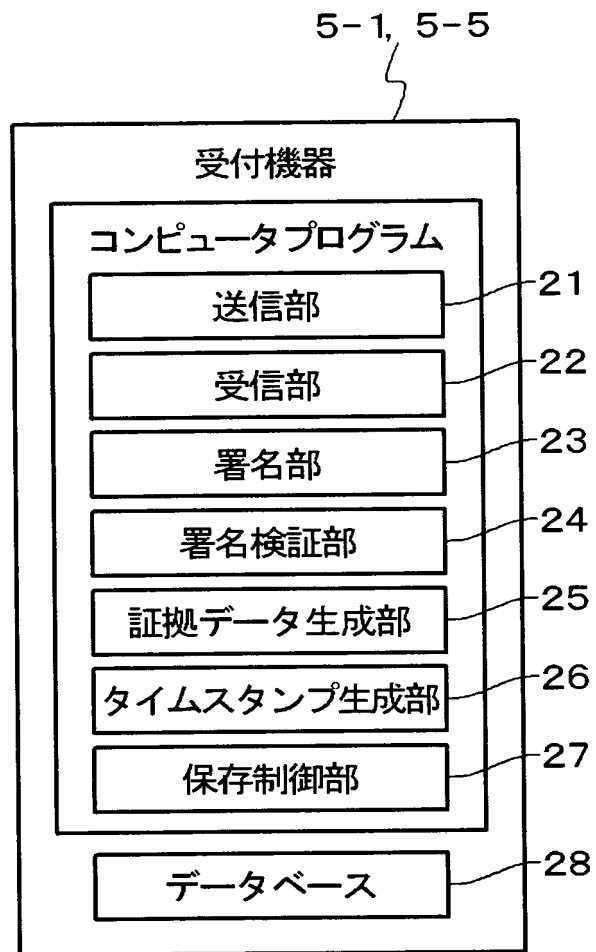
【図 2】



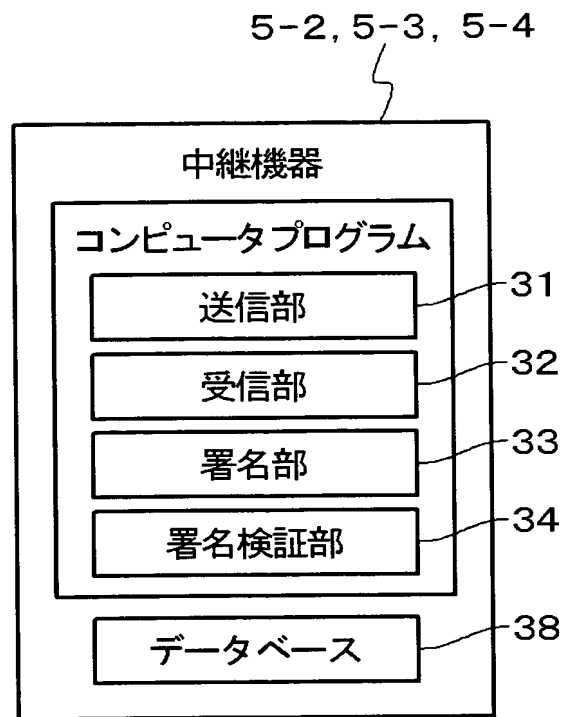
【図 3】



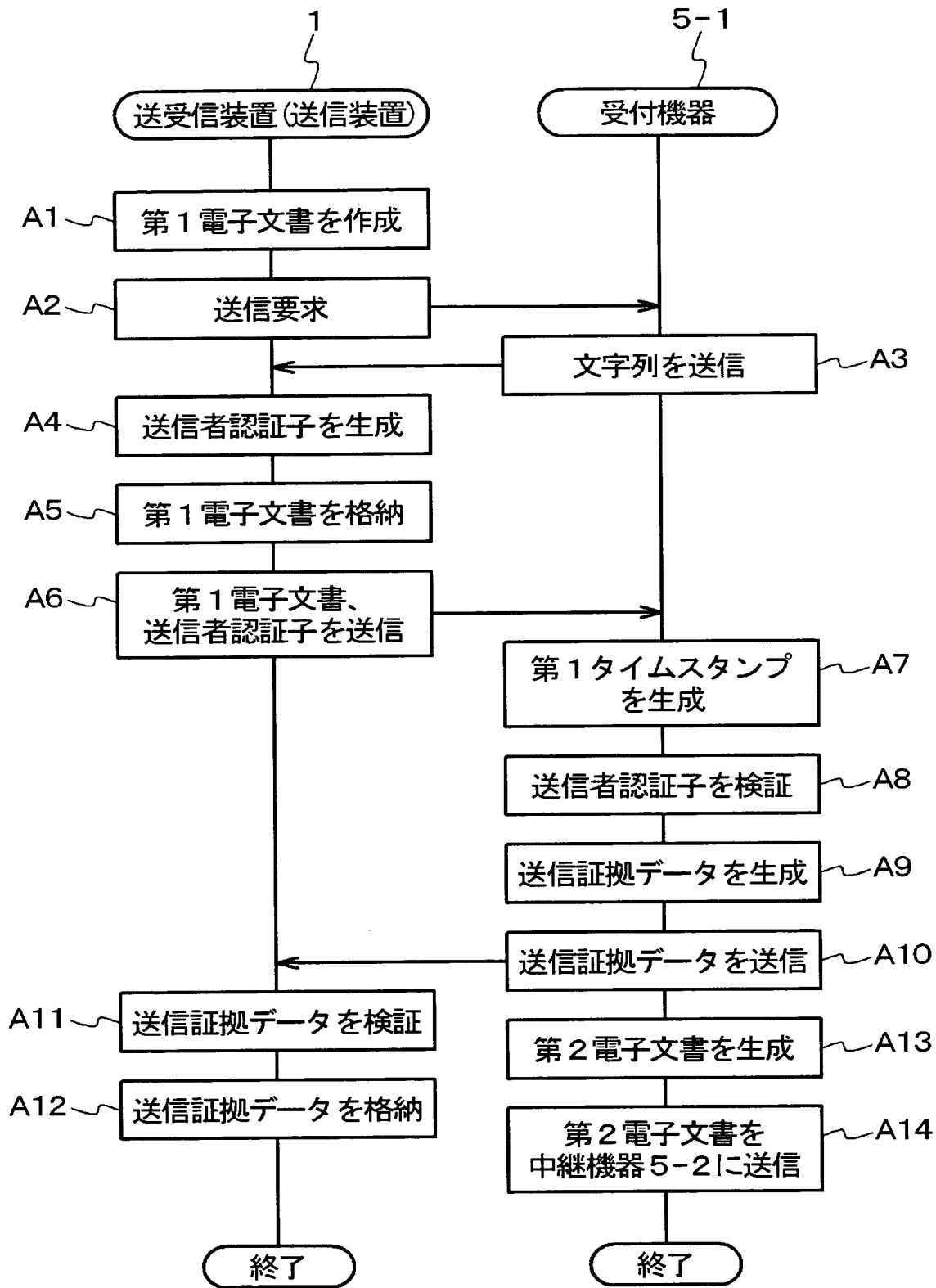
【図 4】



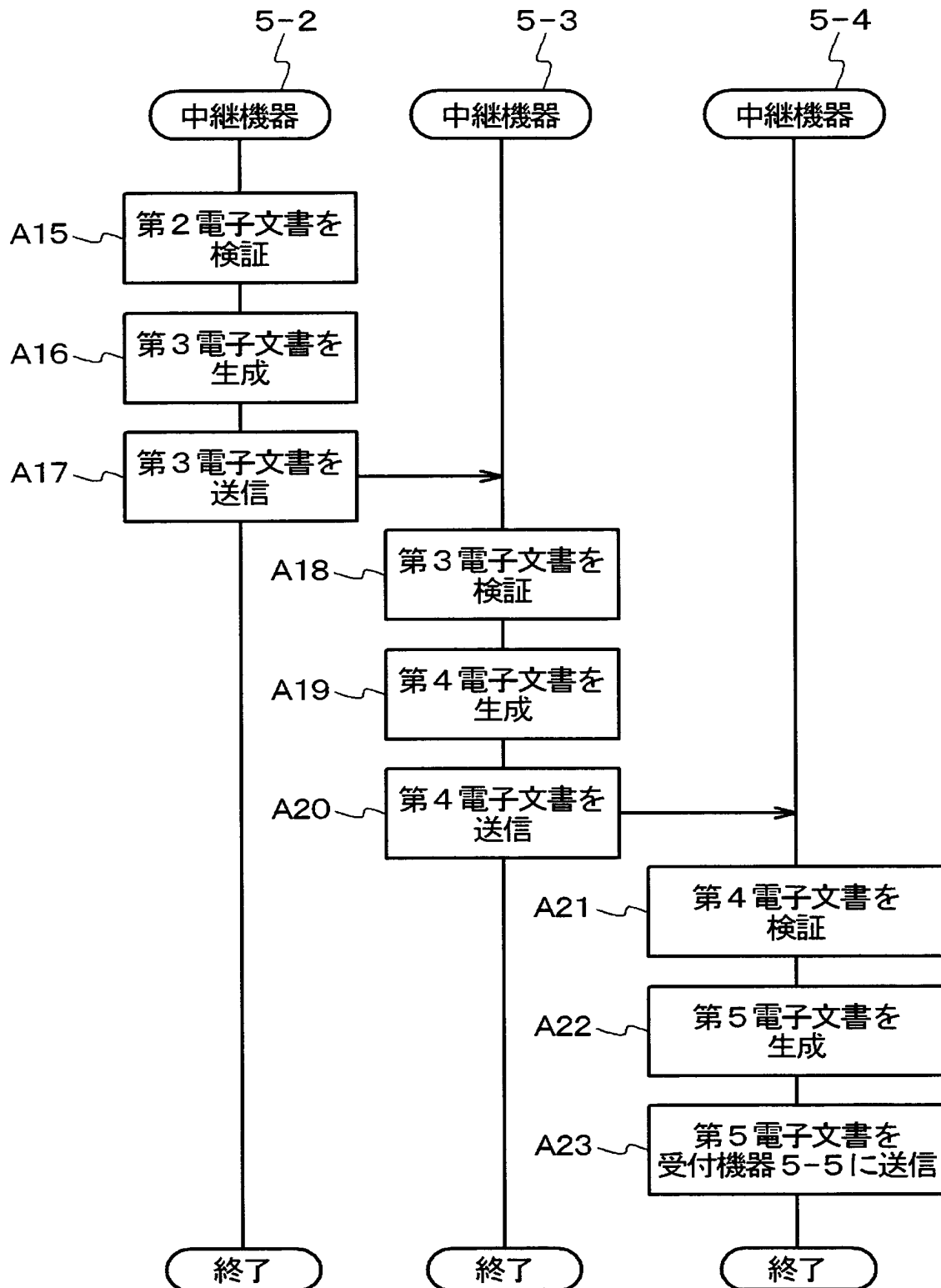
【図 5】



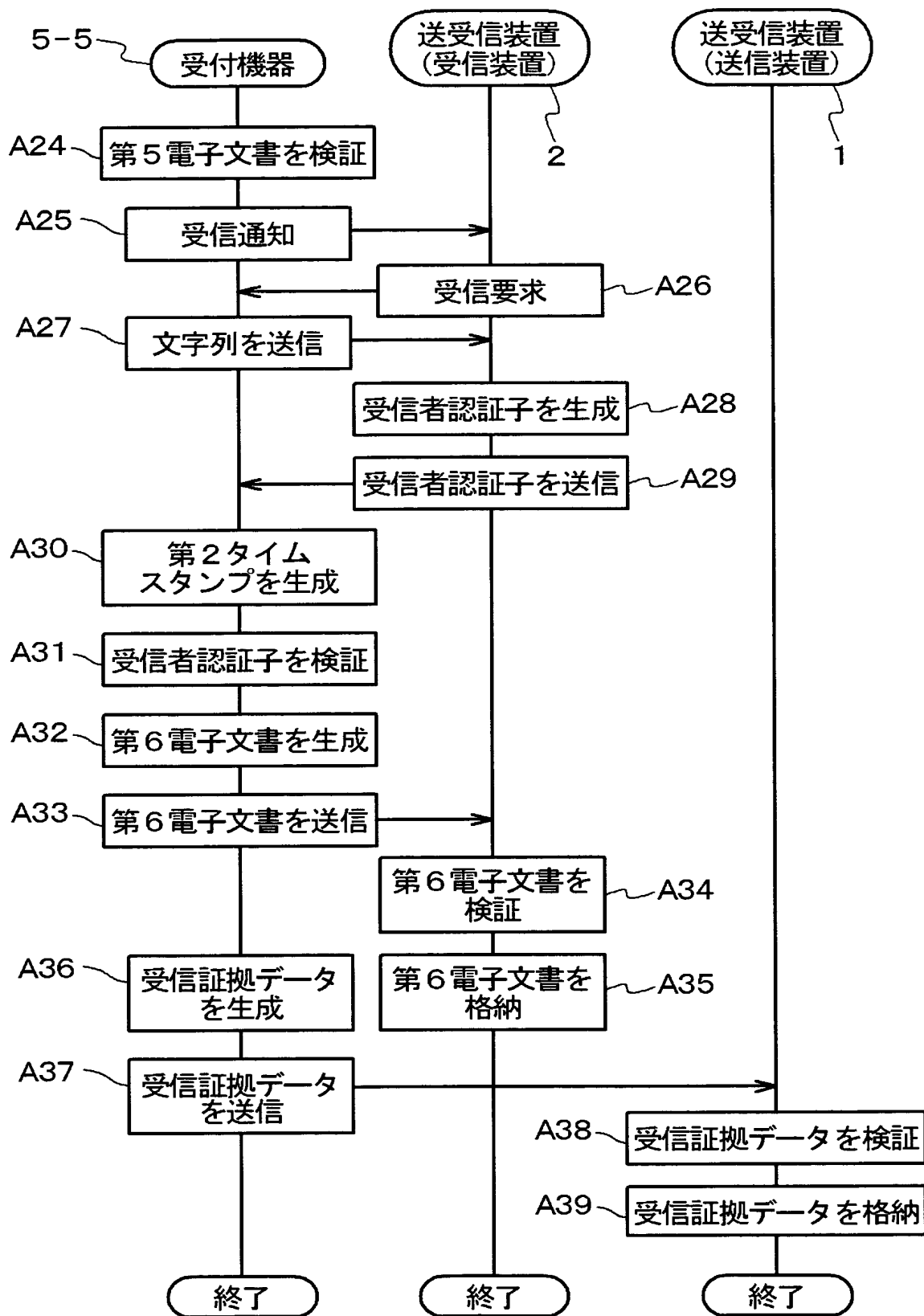
【図 6】



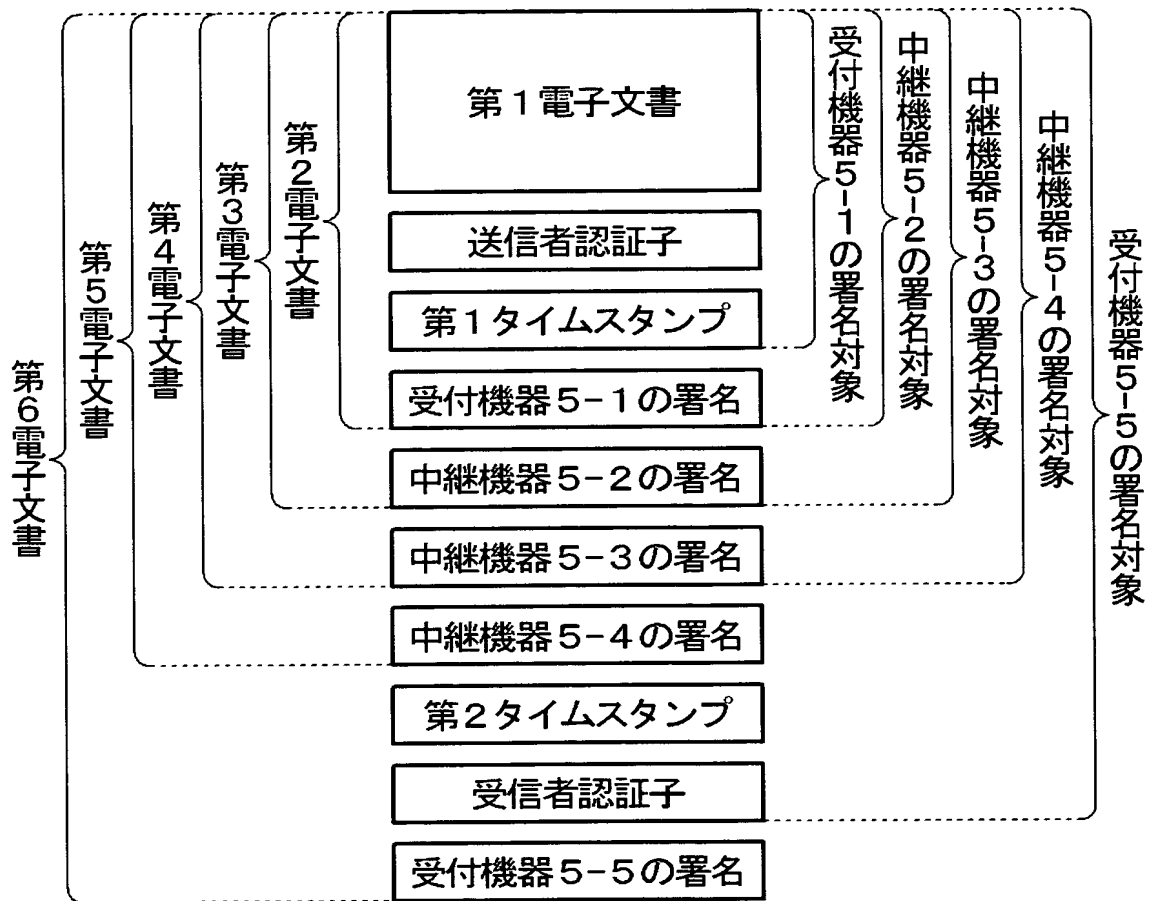
【図 7】



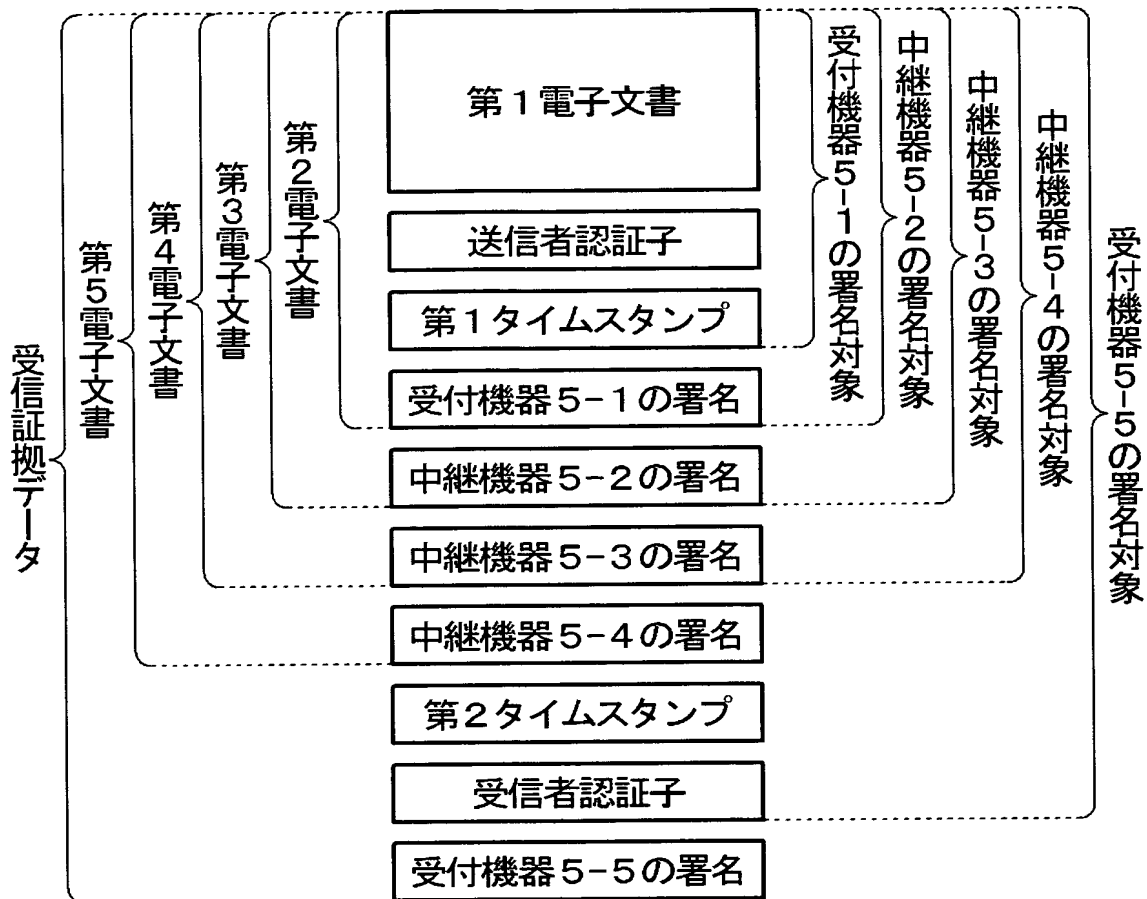
【図 8】



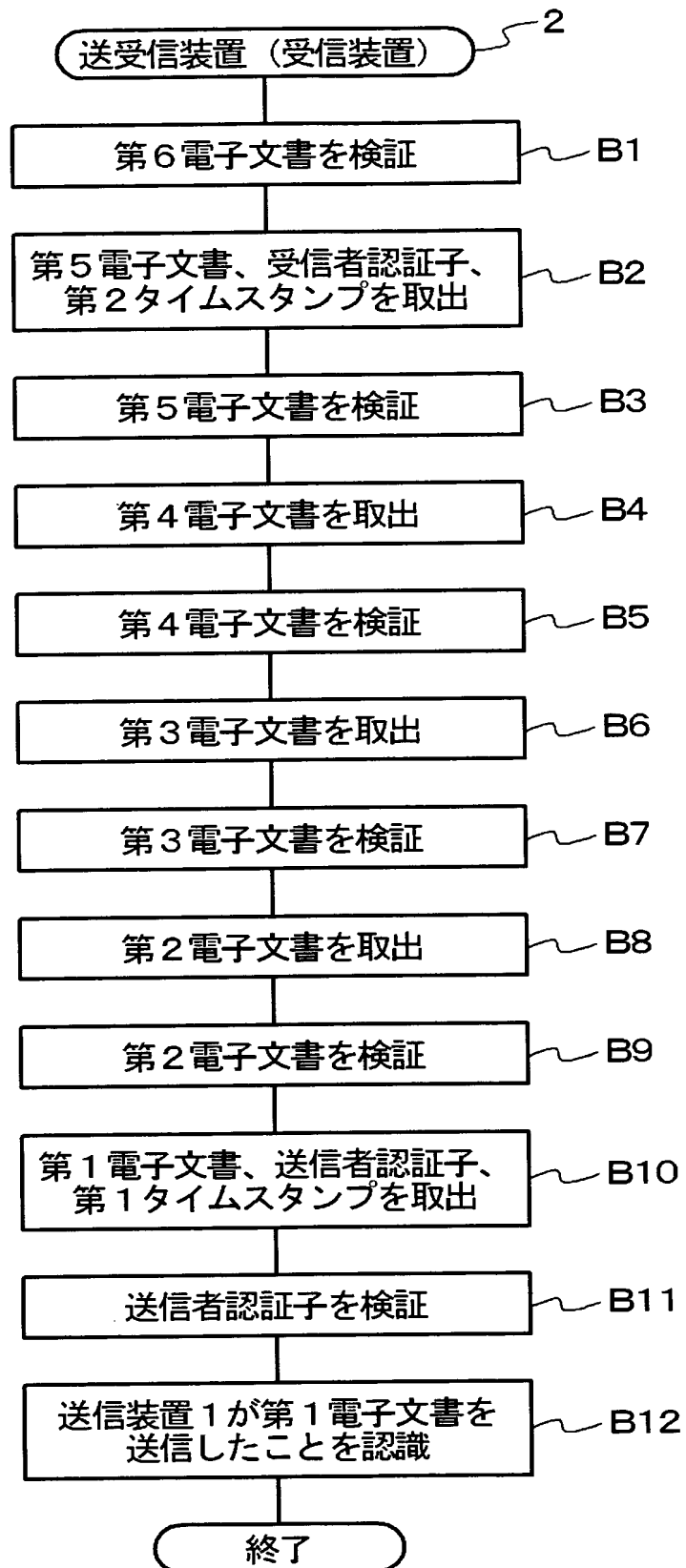
【図 9】



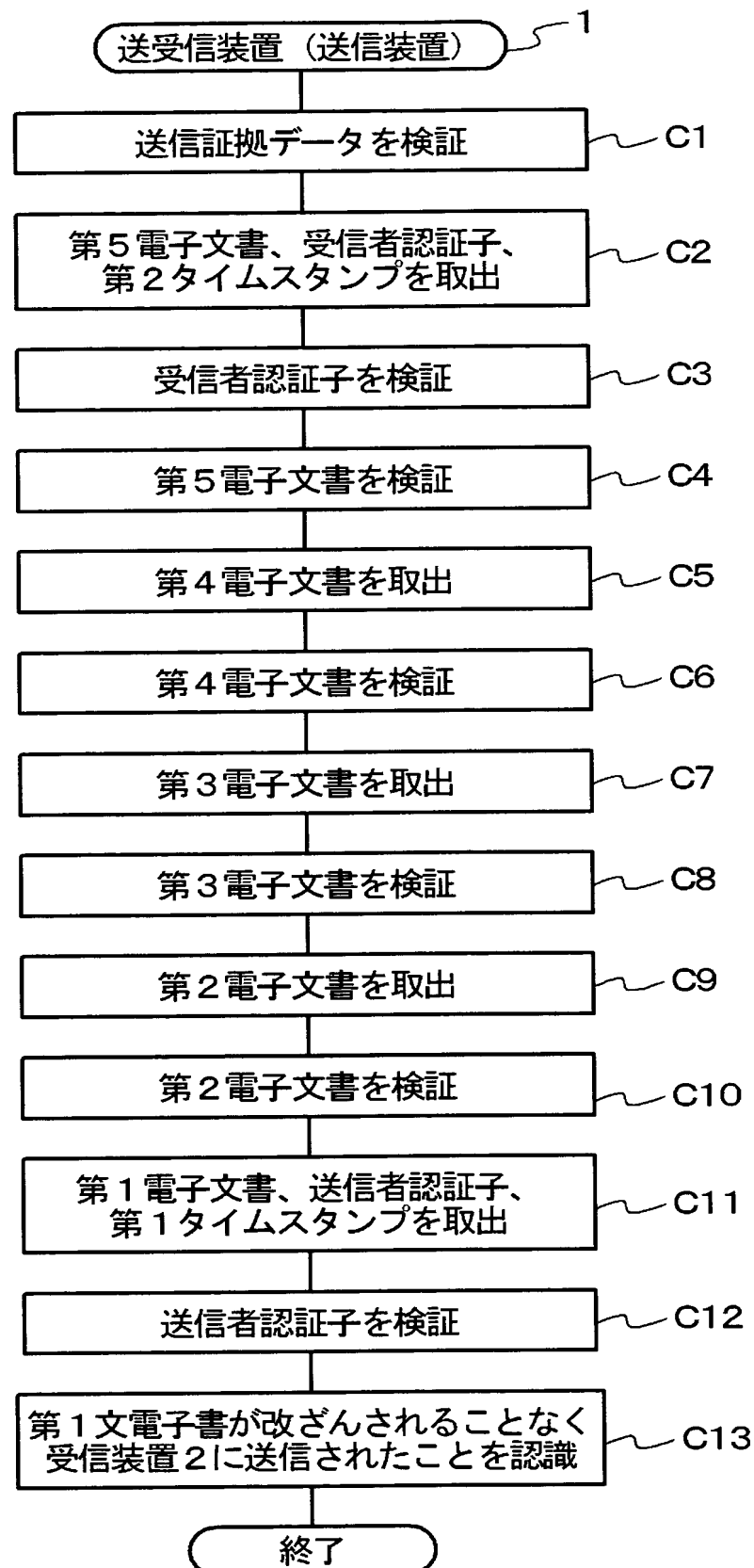
【図 10】



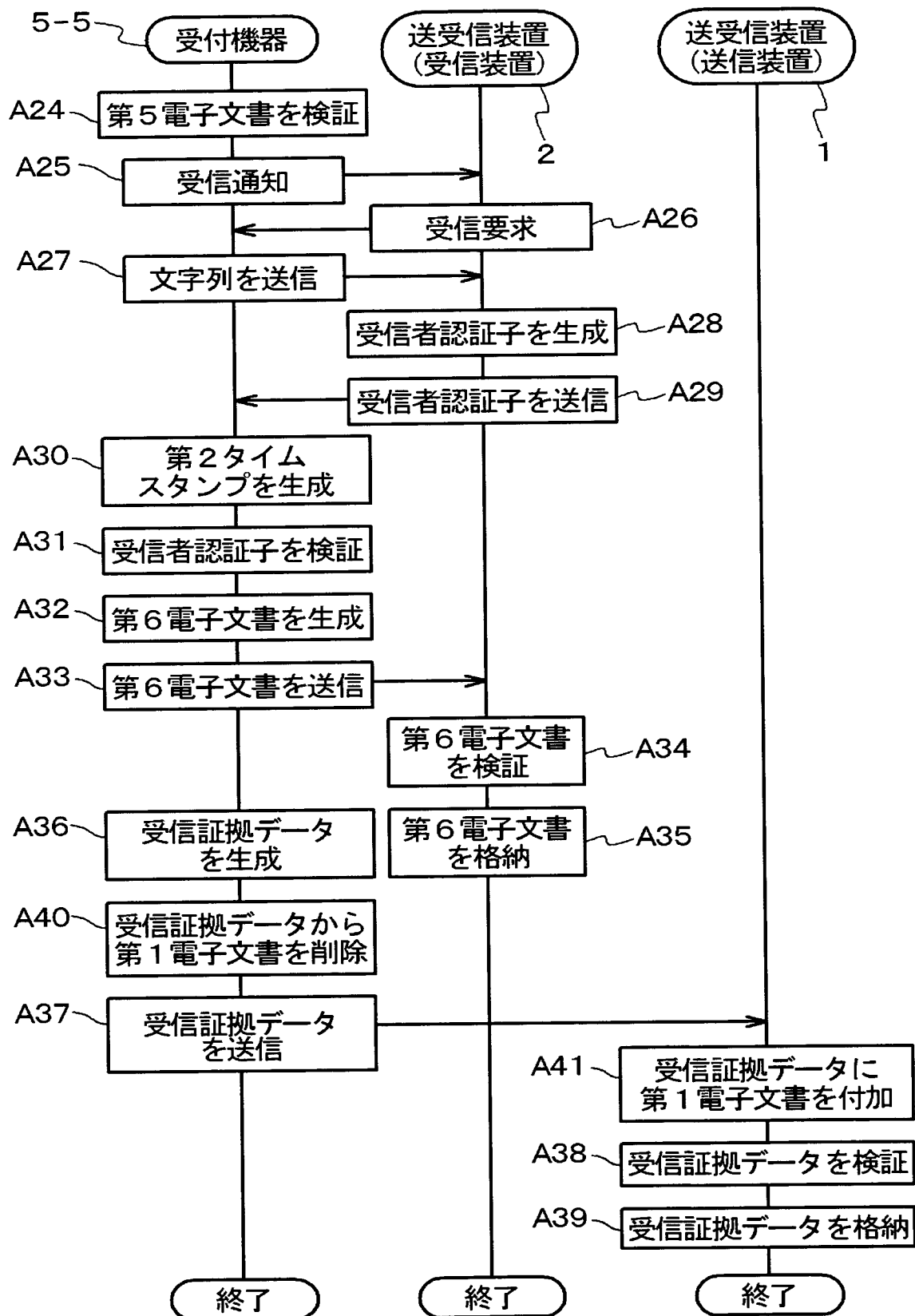
【図 11】



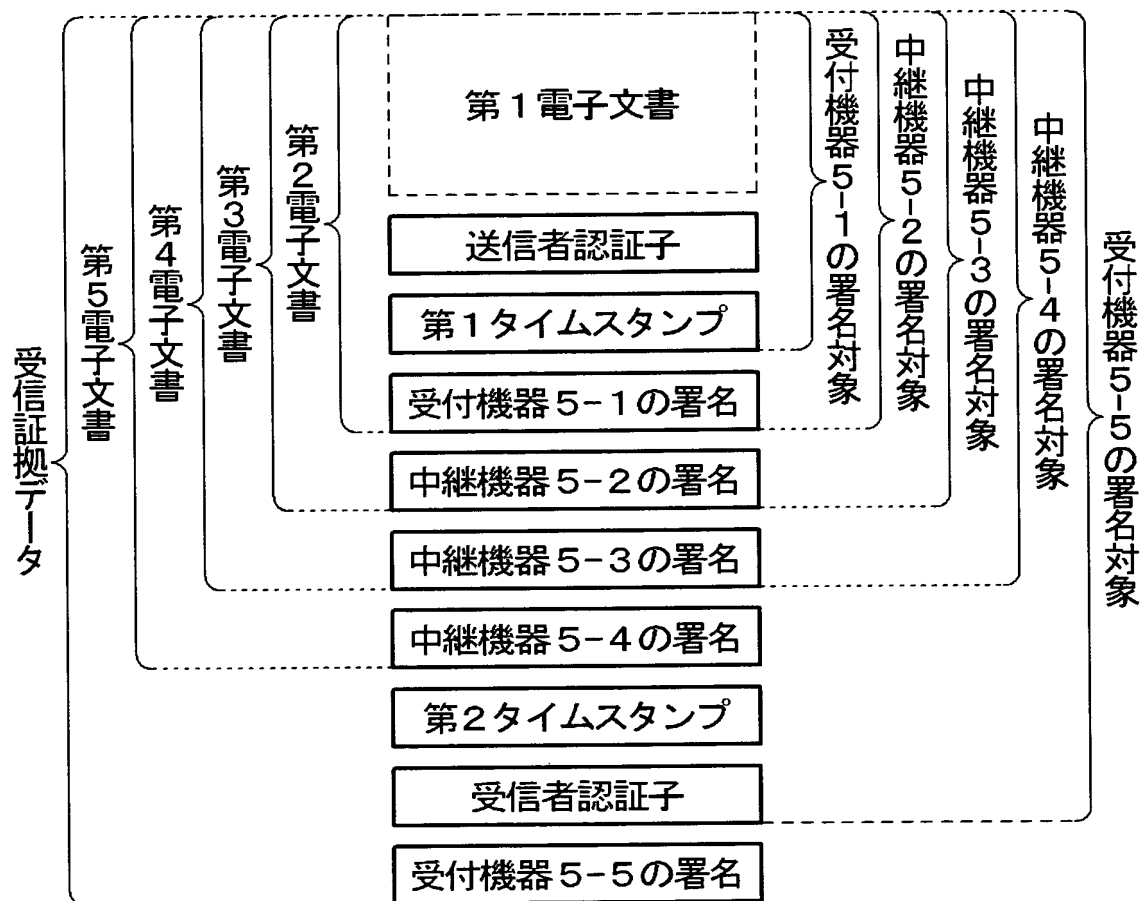
【図 12】



【図 13】



【図 14】



【書類名】 要約書

【要約】

【課題】 送信装置が送信した電子データを受信装置が受信するまで保証する電子データ送受信システムを提供する。

【解決手段】 本発明の電子データ送受信システムは、ネットワーク [100] に接続された n 個の装置 [5-1 ~ 5-n] と送信装置 [1] と受信装置 [2] とを具備する。送信装置 [1] は、第 1 電子データを第 1 装置 [5-1] に送信する。受信装置 [2] は、第 n 装置 [5-n] からの第 $(n+1)$ 電子データを受信する。第 j 装置 ($1 \leq j \leq n$ を満たす整数) は、自己を識別する署名を第 j 電子データに付与した第 $(j+1)$ 電子データを生成して第 $(j+1)$ 装置に送信する。ここで、 j が n のとき、第 $(n+1)$ 装置は受信装置 [2] に対応する。本発明の電子データ送受信システムによれば、第 $(j+1)$ 電子データが生成されるまでに付与された署名により、送信装置 [1] が送信した第 1 電子データを受信装置 [2] が受信するまで保証する。

【選択図】 図 1

特願 2 0 0 2 - 2 9 0 3 8 7

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社